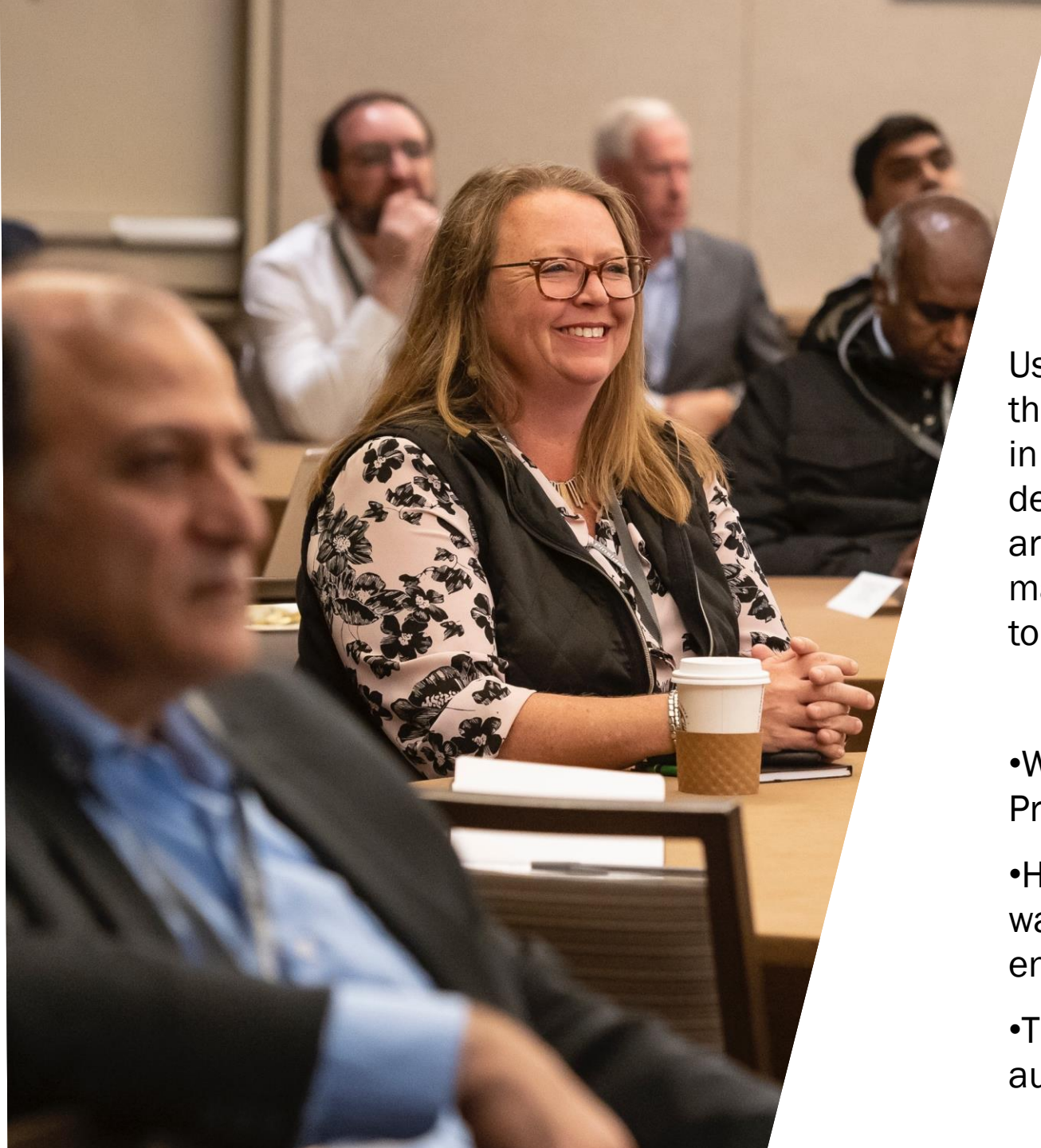




User Provisioning from “Hire to Retire:” How to Streamline, Manage, and Automate User Provisioning

James E. Roeske, CEO
Customer Advisory Group

SAPinsider
2023



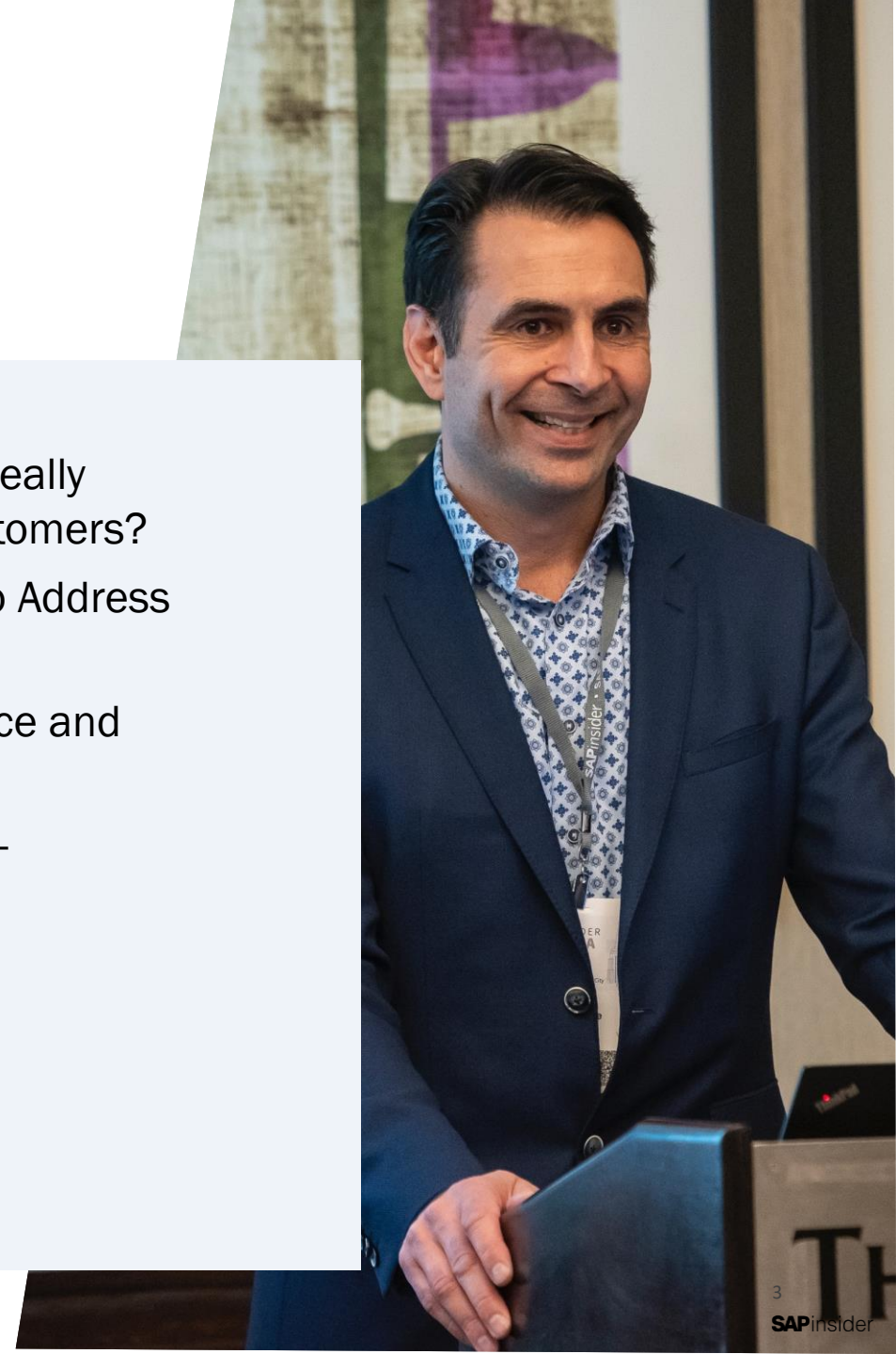
In This Session

User access is a constant and ever-changing process. From the creation of a person's user account, their changing roles in an organization, to the day that the account gets locked or deleted, potentially hundreds of access assignment changes are required. This session provides real world solutions to make sure that people have the right access at the right time to do their jobs.

- Which challenges customer face in the “Compliant Access Provisioning Process”.
- How to facilitate in an efficient, compliant and simplistic way to confront those challenges in today's growing IT environment.
- The many solutions SAP Access Control and IAG provide to automate, control and empower end users

What We'll Cover

- What does “Compliant Access Provisioning” Really Mean, and Why is it Challenging for Most Customers?
- What are the Tools and Processes Available to Address Provisioning Challenges?
- The Holy Grail - Access Provisioning Self Service and Automation
- Making Access Provisioning a One Stop Shop - Connectivity and Integration Options
- Wrap Up



What Does “Compliant Access Provisioning” Really Mean, and Why is it Challenging for Most Customers?

The Prime Directive of a Security Administrator

“Make sure that people have **the Right Access at **the Right Time** to perform their defined and essential job duties. Nothing More and Nothing Less!”**

Sounds easy, right? Unfortunately, it is NOT!

There are many different factors that influence the ability of accomplishing this:

1. The complexity and size of your System Landscape. This includes all the systems your users need to access to perform their job duties. Single System, Cross System, Cross Platform etc.
2. The complexity, structure, and granularity of your security (SAP Role Structure, Naming conventions, number of Roles a person needs to come together to provide the access a person needs)
3. The Tools and processes you have established to allow people to request accesses, or to automatically update Access levels to change as people’s job duties change.



Provisioning Vs. Compliant Access Provisioning



So, what exactly do you mean by “Access Provisioning”?

According to the Security Admin Dictionary: “Provisioning is the execution or assignment of the approved access in the requested SAP system”

That Means:

- Creating consistent user accounts for Users across all systems
- Assigning the right security authorizations/Roles in all systems
- Maintaining User details such as Name, Email, Phone Numbers, Addresses etc...
- Maintaining passwords – Initial, resets or SSO SNC details
- Removing access for position changes and terminations
- Locking and deleting accounts in all systems to prevent inappropriate access after off-boarding

What is “Compliant Access Provisioning” than?

That Means – ALL of the “Provisioning tasks” PLUS:

- Maintaining a consistent process and audit trail for all provisioning actions
- Performing risk analysis and assign Mitigating Controls for User access which causes compliance conflicts or risk
- Obtain and document approvals for access assignments and all other security changes
- Facilitate constant and consistent User Access Reviews to prevent inappropriate or obsolete access assignments
- Monitor/Log Emergency Access Usage

Provisioning Workloads and Complexity are Increasing



“Back in the old days when I started in SAP I only had to worry about ONE R/3 Landscape (Dev, QA, and PRD). People would send me an email, or pick up the phone and call me to discuss a security issue. I would then “Fix it”.

Times have changed!

“Now, I need to worry about ELEVEN different SAP Landscapes today with some users needing access to a combination or all eleven systems. I also need to have everything documented for the Auditors, check for segregation of duty issues, assign Mitigations, obtain approvals for changes....and that is only in SAP, it does not include the new Cloud Applications we are in the process of implementing and and the Non-SAP systems that I need to administer!!!!”

Type of System	System	Client	Notes/Requirements	Type of System	System	Client	Notes/Requirements
ECC	PRD(1)(2)	700	(1) Tolerance level, (2) purchasing group	Solution Manager	SMD(6)		Production (6) Business Partner must be setup
	QAS	700			SMX		Development
	DEV	200 & 700		GRC	GRP		
	SND	700	Sandbox (limited to IT in RBAC)		GRD		
APO	APP			Fiori	GWP		
	APQ				GWQ	200	Client 200 on GWD box
	APD				GWD	100	
	APS		Sandbox (limited to IT in RBAC)	Enterprise Portal	EPP		
BW	BWP(3)		(3) Notification sent to training		EPQ		
	BWQ				EPD		
	BWD			DMF	DMP		IT only as part of RBAC
CRM	CRP(4)(5)		(4) Maintain parameters, (5) CRM exception for credentials – send credentials to CRM setup DL		DMQ		IT only as part of RBAC
	CRQ				DMD		IT only as part of RBAC
	CRD			BOBJ	BOBJP		Part of BW
BPC	BPC Prod		Provisioned through BW?		BOBJQ		Part of BW
	BPC QA		Provisioned through BW?		BOBJD		Part of BW
	BPC Dev		Provisioned through BW?				

The Evil Evolution of User Access with Poor Provisioning Processes

- Security Admins Giveth Access, and Taketh Away! (Well, most of the time!)



- It is very easy to give access.
- Manager said they need it, so we give it.

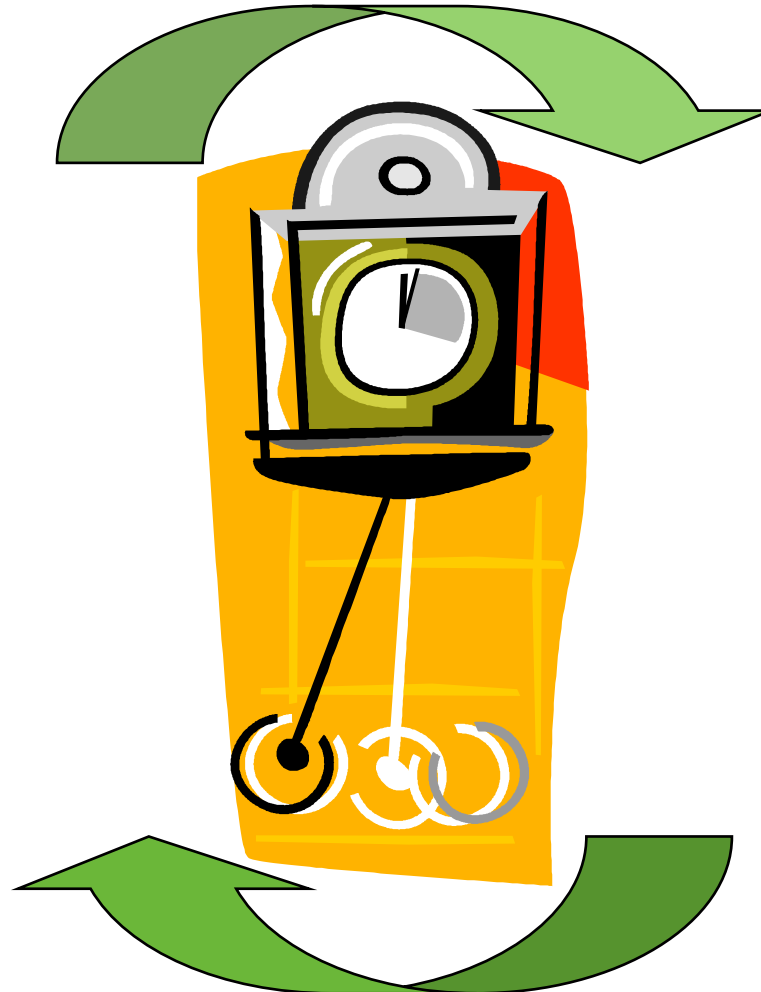


- But not as easy to take it away.
- Are they using it, is it critical for their job?

Stop the Security Cleanup Pendulum

Goal: Eliminate the Security Clean-Up Pendulum Effect

**Take Access Away to
“Cleanup” User
Access and Eliminate
all SoD Violations**



**Have to Give the
Access
Back Because the
Business Can No
Longer
Function!**

The Evil Evolution of User Access with Poor Provisioning Processes

- Sally has worked for the company for 27 years, she started in HR, then moved to Procurement, and is now running Finance



- **You Trust Sally with all that Access ... right?**
- **You also Trust Sally's replacement who sends an access request for "I NEED what Sally has" ... right?**



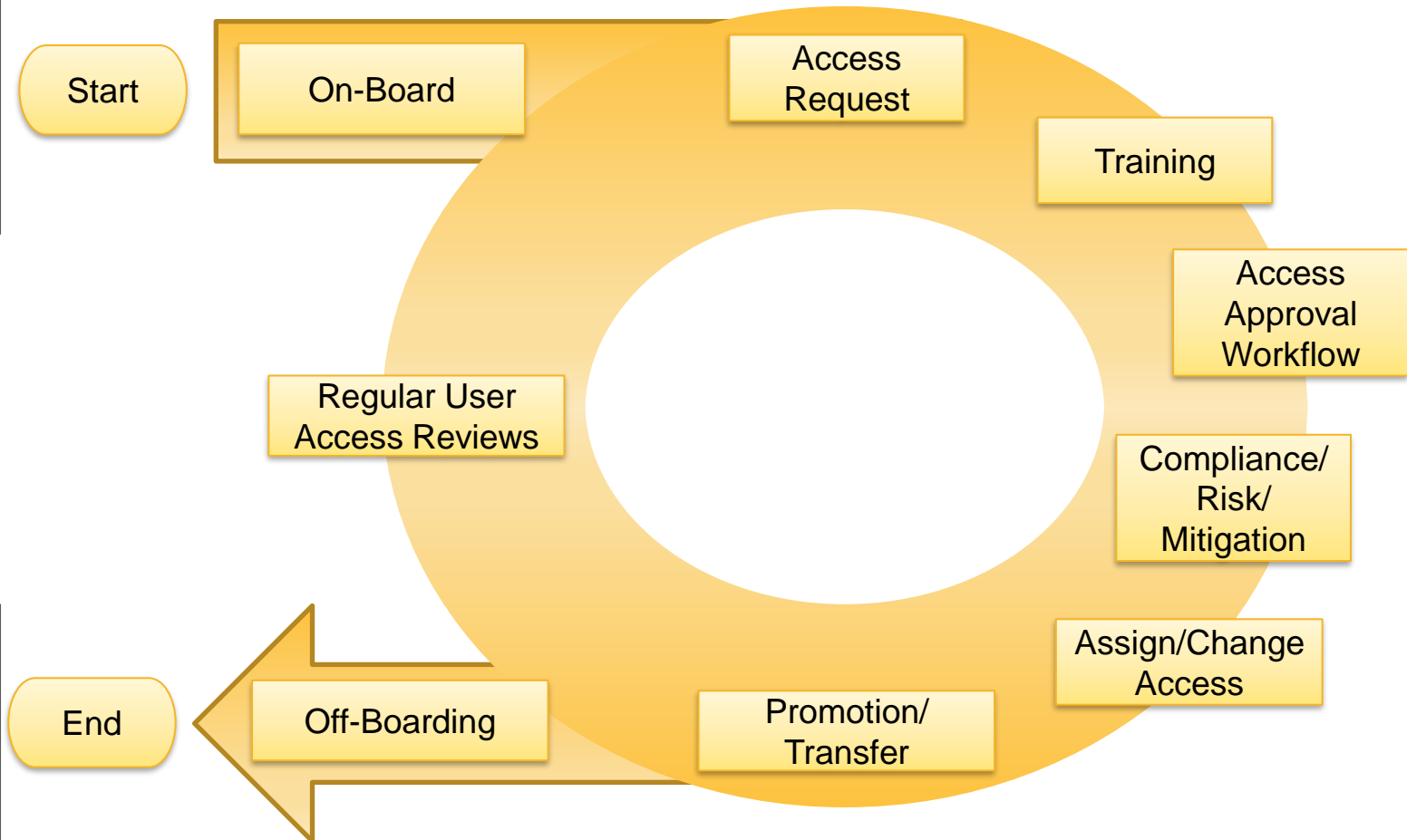
With the accumulation of all the access over the years, Sally basically has "SAP almost, kind of, sort of ALL"!

The Goal - User Compliant Provisioning Life Cycle

The Circle of Life in an
Ideal Compliance
Provisioning World!

Are you Following this
Cycle?

Are These Steps Manual
or Automated in your
Company?



Compliant Provisioning is NOT just a one-time task for Security Admins

- In a healthy security environment, employee access needs to reflect their current job tasks
 - Therefore, as their tasks change over time so should their access levels. This mean there should be processes in place to remove “un-needed” and “risky” access.
 - User Access Reviews as an excellent way to have consistent monitoring access decisions made by owners outside the security team



- **It should not be the security team's job to know when people need access removed or decide what access people need**
- **The business knows best, they MUST be involved!**

The Formula for Better Provisioning and Return on Investment



Self Service:

Getting users to participate in Requesting their own access and participating in compliance processes

Automation:

Letting the system do the “Heavy Lifting” by Managing Access Requests, Approvals, Risk identification and provisioning the access in the Systems

Reduce effort increases ROI:

Admins can focus on their real jobs rather than the “Clicky Clicky” work of day to day Access Provisioning

Why Do Security Admin's do most of the Provisioning "Heavy Lifting" today?

- Top 5 reasons from customers why Admins are so heavily involved in day to day security and compliance end user tasks:
 1. Security is too Complex! It would take too long to teach our end users. I'm the "Security Rosetta Stone", I know or can figure out Security needs better and faster.
 2. They don't care, we don't trust them to do the right thing when requesting Access!
 3. The Access Request system is too complex or "user Un-friendly" for our End Users.
 4. Good Customer Service! I will do all I can to make their lives easier!
 5. It's my job not theirs.....What would I do all day if they did need me?

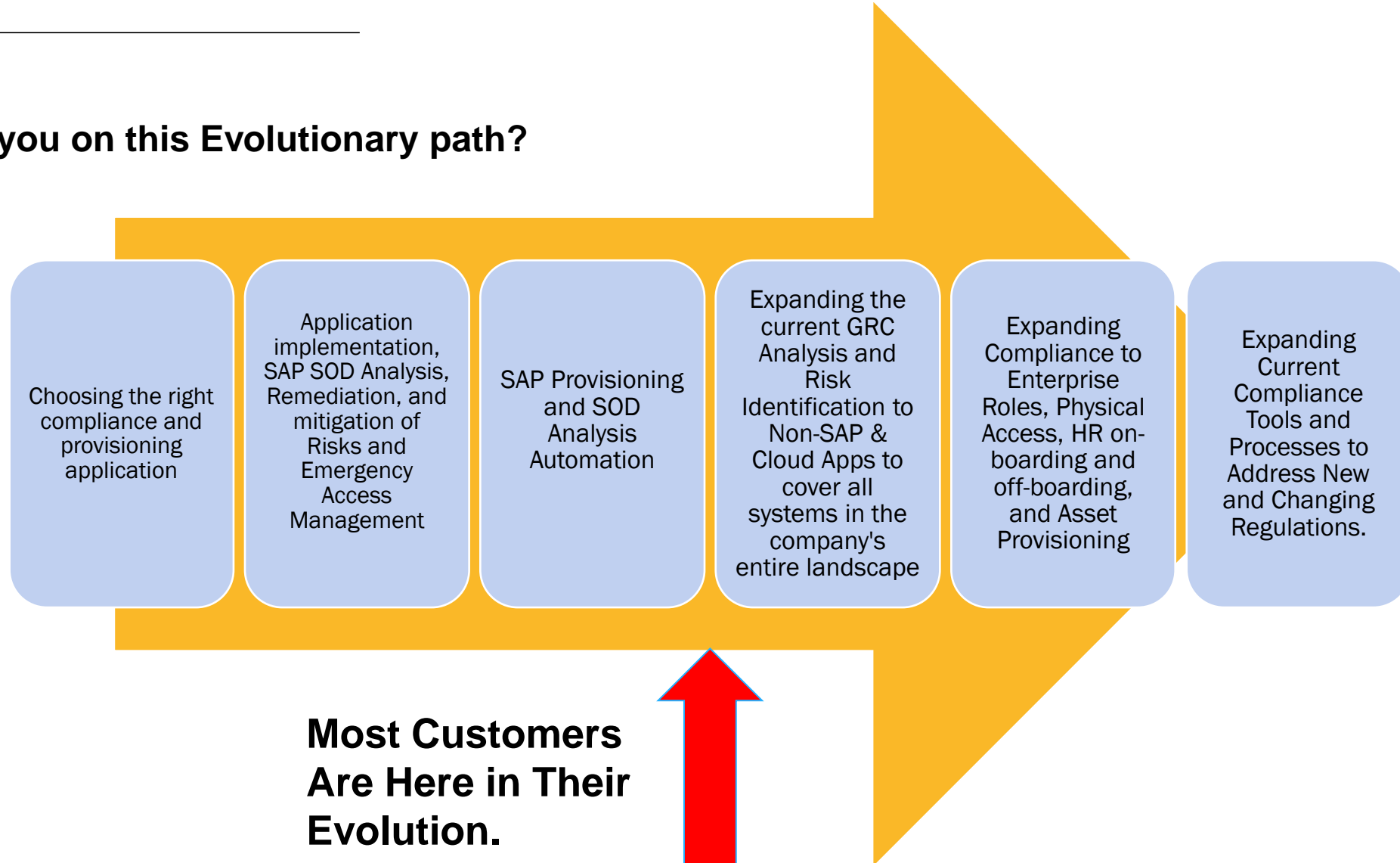


What are the Tools and Processes Available to Address Provisioning Challenges?







The Evolution of a Typical SAP Customer for Compliant Provisioning

Where are you on this Evolutionary path?



SAP Products to Address Provisioning and Compliance Challenges

SAP GRC and Security solutions

 Enterprise Risk & Compliance	 Identity & Access Governance	 Cybersecurity, Data Protection & Privacy	 International Trade Management
<ul style="list-style-type: none">✓ SAP Process Control✓ SAP Risk Management✓ SAP Audit Management✓ SAP Business Integrity Screening✓ SAP Regulation Management by Greenlight	<ul style="list-style-type: none">✓ SAP Access Control✓ SAP Cloud Identity Access Governance✓ SAP Access Violation Management by Greenlight✓ SAP Dynamic Authorization Management by NextLabs✓ SAP Single Sign-On✓ SAP Cloud Identity Services – Identity Authentication✓ SAP Identity Management✓ SAP Cloud Identity Services – Identity Provisioning	<ul style="list-style-type: none">✓ SAP Enterprise Threat Detection✓ SAP Privacy Governance✓ SAP Privacy Management by <u>BigID</u>✓ SAP Customer Data Cloud✓ SAP Data Custodian✓ SAP Data Custodian, Key Management Service (KMS)✓ UI masking for SAP✓ UI logging for SAP✓ SAP Code Vulnerability Analyzer✓ SAP Fortify by Micro Focus	<ul style="list-style-type: none">✓ SAP Global Trade Services✓ SAP S/4HANA for international trade✓ SAP Watch List Screening



That is a lot of GRC functionality!

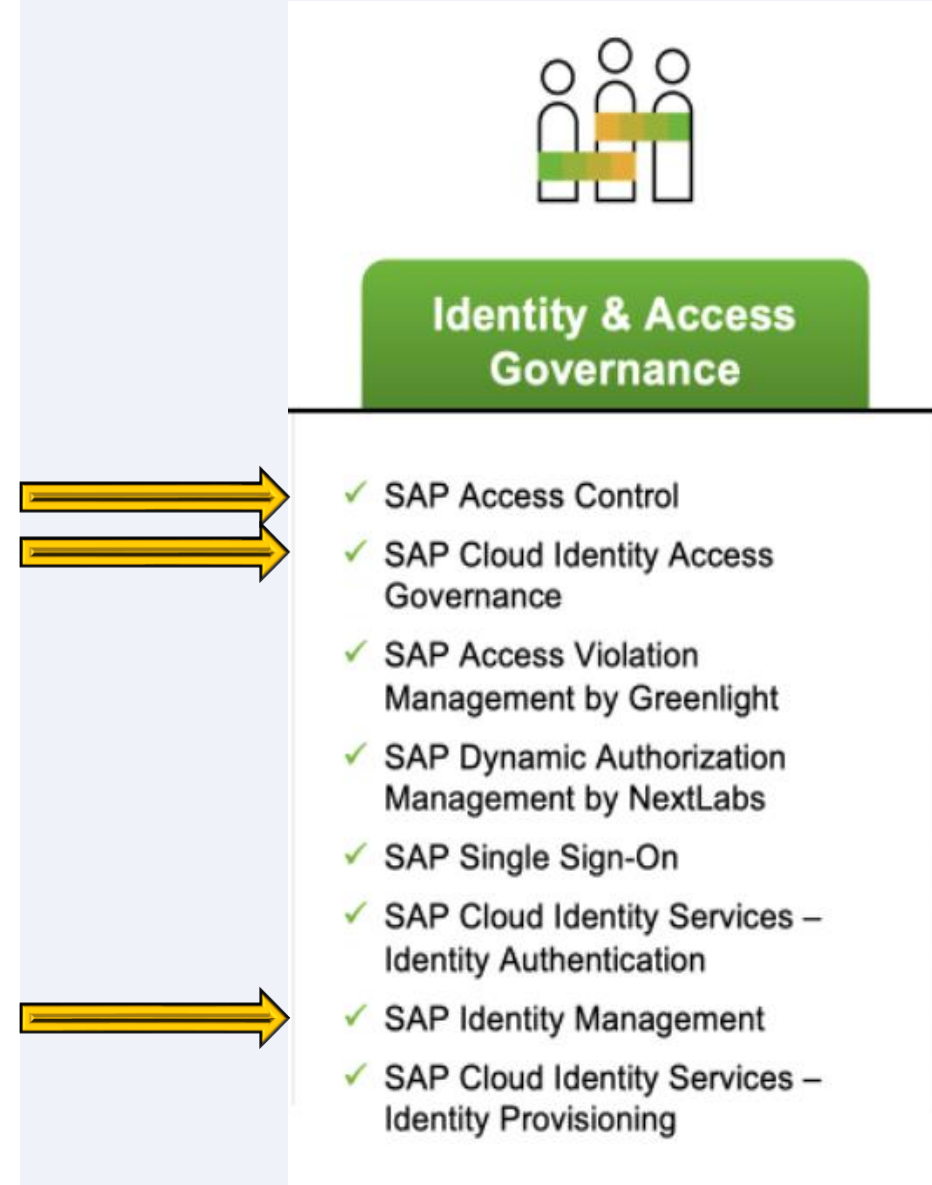
I didn't even know that half of these SAP products existed!!!

Don't these SAP Products all do the same thing – No, No They Don't!






















With the SAP GRC Product Portfolio there are multiple products that were specifically built to help customers with both the challenges of “Provisioning” and “Compliant Provisioning”.

The key Products we will be focusing on are

- SAP Identity Management
 - SAP Access Control
 - SAP Cloud Identity Access Governance
 - AND - How they can Integrate and potentially work together
-
- Please Note – There are also many other IDM Products on the Market that can also Integrate with the SAP GRC applications to provide a wholistic “Compliant Provisioning Solution”

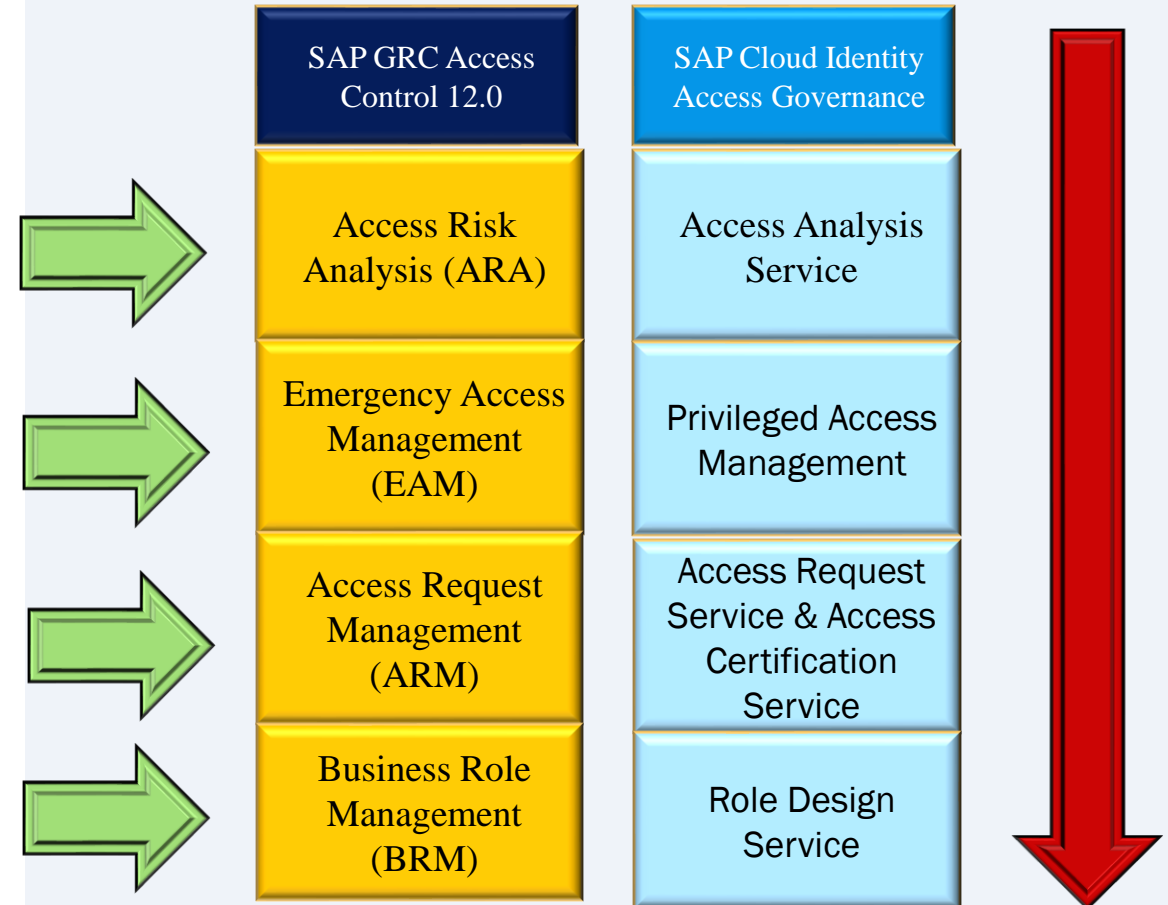


Product Comparison

	SAP Identity Management	SAP GRC Access Control	SAP Cloud Identity and Access Governance
Analyze Risk			
Privilege Access Management			 Recent Addition
Role Design			
Access Request			
Central Identity Store			
Access Certification			 Recent Addition
Flexible/ Configurable Workflow			 Future Release

GRC for Compliant Provisioning

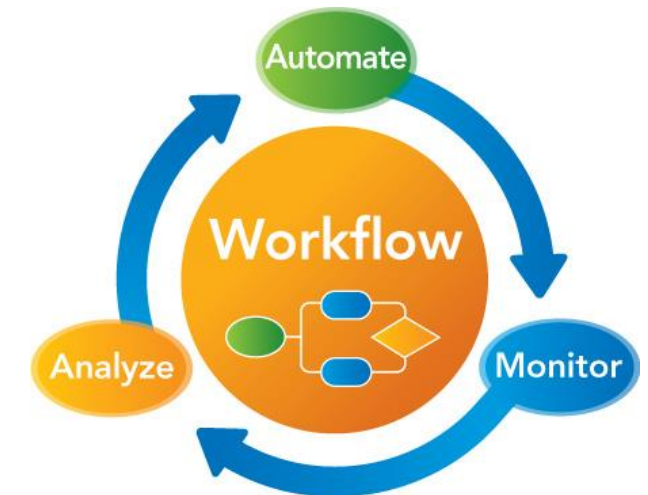
- Most critical application for compliance related to SoD's. As well as very important for risk analysis to be integrated within other SAP Access Control components.
- Quick and easy to configure and get up and running. Can instantly solve outstanding audit points related to excessive access levels. Speedy return on investment.
- Key component for "Continuous Compliance" and enforcing proactive SOD checking rather than reactive. Primary mechanism for automating the provisioning process. This component will provide additional benefit AFTER the initial "Clean-up and mitigations" of SOD issues have been completed.
- Enables the enforcement of a consistent Role creation, maintenance and documentation process for Security Roles. Provides direct simulation and SOD checking to provide proactive SoD prevention during role development and maintenance.



Compliant Provisioning – SAP GRC Access Control - Access Request Management

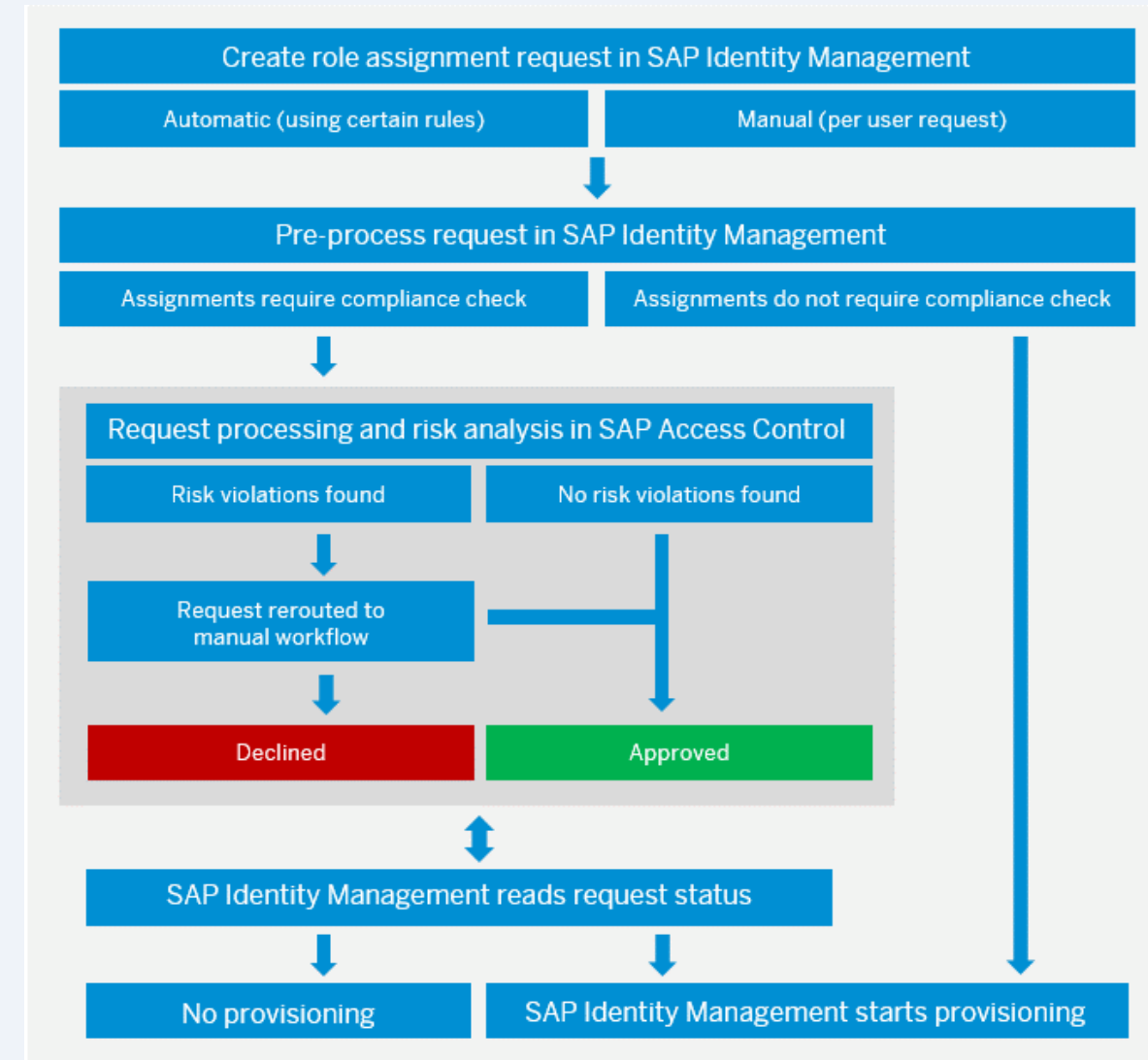
I call it the “Automation” part of SAP Access Control

- Access Request Management is an automated user request, approval, and compliant provisioning solution which is workflow configurable with proactive SoD compliance checking.
- Integration with SAP HR/SuccessFactors for HR Triggered automatic Access Requests for New Hire, Position Change, and Termination scenarios
- Is the main engine for User Access Reviews and SoD Review functionality
- Facilitates Password Self-Service
- Facilitates all Workflow enablement for the other Access Control applications including EAM log Reviews, ARA Mitigation and Rule set Change Control Approvals



IDM and GRC Working Together - Centralized Provisioning

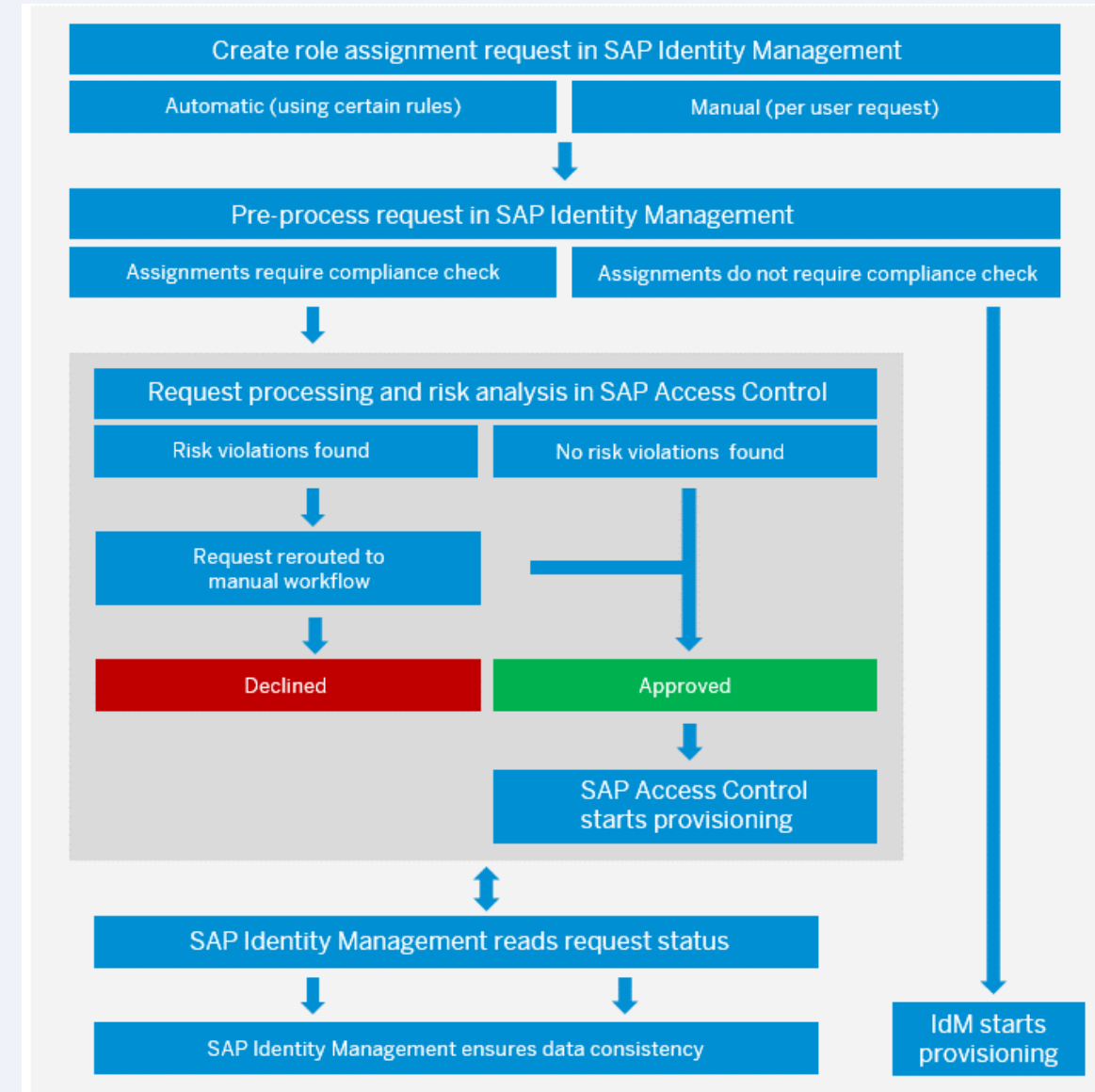
This is a scenario where SAP Identity Management is the only provisioning system, responsible for provisioning both the assignments that require and do not require compliance checks to the target systems (both SAP and non-SAP).



IDM and GRC Working Together - Distributed Provisioning

This is a scenario where the provisioning is performed both by SAP Identity Management and SAP Access Control. SAP Identity Management is responsible for provisioning the assignments not requiring compliance checks to multiple target systems (both SAP and non-SAP), while SAP Access Control is used for provisioning assignments requiring compliance checks to SAP ABAP target systems (usually a request to SAP Access Control that may require manual approval). This means that no ABAP repositories (and the associated privileges) exist in the Identity Management.

Source: SAP



SAP GRC Access Control Webservices



GRC has standard available webservices that allow IDM and potentially other applications to Retrieve and Pass information to SAP Access Control for the purposes of User Access Requests, SoD Risk Analysis, and even Security Role lookup information.

Screenshot from SAP GRC Access Control System:

SE80 > Package > GRAC_DIRECTORY_SERVICES > Expand Enterprise Services > Service Definitions.

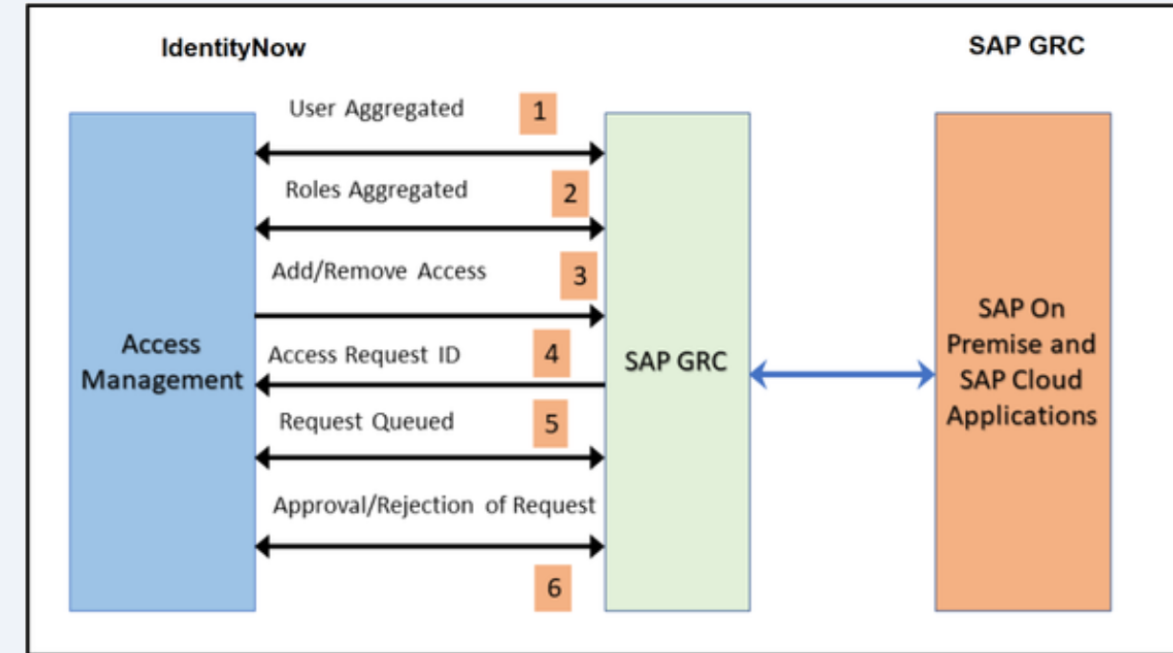
	Object Name
<input type="checkbox"/>	> Dictionary Objects
<input type="checkbox"/>	> Class Library
<input type="checkbox"/>	> Programs
<input type="checkbox"/>	> Function Groups
<input type="checkbox"/>	> Includes
<input type="checkbox"/>	> Transactions
<input type="checkbox"/>	> Message Classes
<input type="checkbox"/>	▼ Enterprise Services
<input type="checkbox"/>	▼ Service Definitions
<input type="checkbox"/>	GRAC_AUDIT_LOGS_WS
<input type="checkbox"/>	GRAC_EUP_CONFIG_DATA_WS
<input type="checkbox"/>	GRAC_EXIT_FROM_IDM_WS
<input type="checkbox"/>	GRAC_FIRE_FIGHTER_WS
<input type="checkbox"/>	GRAC_LOOKUP_WS
<input type="checkbox"/>	GRAC_ORG_ASSGN_REQUEST_WS
<input type="checkbox"/>	GRAC_PROV_LOGS_WS
<input type="checkbox"/>	GRAC_REQUEST_DETAILS_WS
<input type="checkbox"/>	GRAC_REQUEST_STATUS_WS
<input type="checkbox"/>	GRAC_RISK_ANALYSIS_WITH_NO_WS
<input type="checkbox"/>	GRAC_RISK_ANALYSIS_WOUT_NO_WS
<input type="checkbox"/>	GRAC_ROLE_DETAILS_WS
<input type="checkbox"/>	GRAC_SEARCH_ROLES_WS
<input type="checkbox"/>	GRAC_SELECT_APPL_WS
<input type="checkbox"/>	GRAC_USER_ACCES_WS
<input type="checkbox"/>	GRAC_USER_EXISTING_ASSGN_WS
<input type="checkbox"/>	> RFC Services

IDM and GRC Working Together – Other IDM Vendor Products Distributed Provisioning

The SAP GRC Webservices can not only help integrate SAP Products but can also be leveraged by other IDM Vendors to Capitalize on SAP Access Controls Strengths for Compliance and Provisioning while linking an existing IDM request process process and application.

Each number in the diagram represents one of the following processes:

1. User aggregated from GRC connected system.
2. Roles aggregated from GRC connected System.
3. Request sent to add / remove access to connected System.
4. Access Request ID created in GRC.
5. Request waits in IdentityNow queue until a response is issued by SAP GRC.
6. On the basis of the response returned from SAP GRC (approval or rejection in GRC), SAP GRC would provision or reject the request and corresponding status would be maintained in the SAP GRC source.



The Holy Grail - Access Provisioning Self Service and Automation

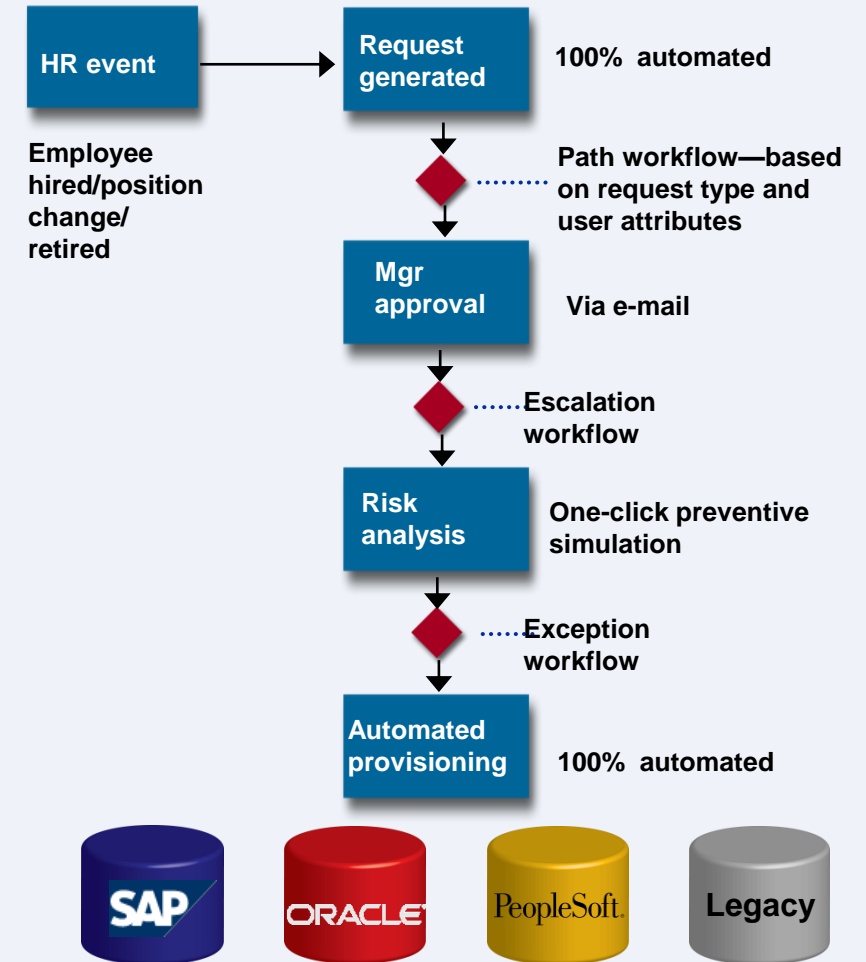


HR Triggers – Request Automation

The ability to setup automatic workflow requests based on a function/action that occurs in an HR system

Enables compliant end-to-end provisioning
“hire to retire”

- Embed **cross-enterprise preventive compliance** in business process
- **Reduce cost** of user administration
- **Improve productivity** of end users
- Provide **auditable tracking** for auditors

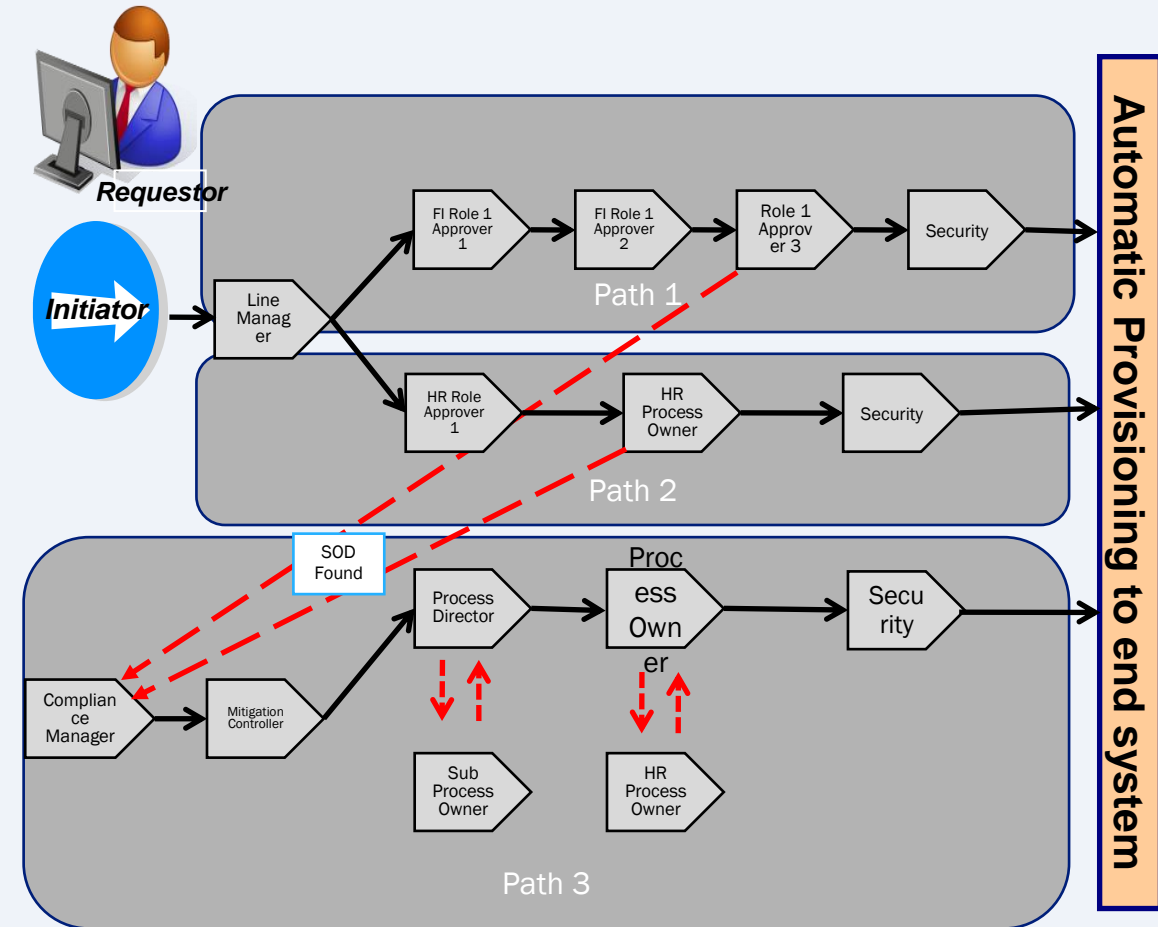


Identity & Access Compliance – Business Ownership Involvement and Participation

It isn't until Customers have gotten over the hurdle of the initial stages of their compliance “evolution” with GRC Access Control that they see that it contains functionality and tools that allows for some key Compliance and Security task to be Automated or taken off the shoulders of “Administrator” and “Help Desks” and put in the hands of the people in the trenches.

Examples:

- Self service access request form submission
- Workflow Driven User Access Request Processes that are “pushed” to Business Owners
- Approvals and automatic audit trails centrally captured in the GRC system
- Password Self Service functionality and automated password provisioning
- Automating provisioning of access at the end of an GRC ARM request
- Automated FireFighter assignment provisioning
- Automatic SoD checking during a ARM User access request or BRM role change



The Future – Augment Access Control

PROJECT BRIEF

Augmented Access Control *Recommender*

Smart access request
recommendations for
simpler and more
secure access

Problem Space

- **Business users struggle** to understand and identify which authorization roles provide required access to the systems needed for completing their work
- **Request approvers struggle** to understand the context behind requests when making risk assessments, as request reason is often left blank or non-descriptive in access requests

© 2022 SAP SE or an SAP affiliate company. All rights reserved.



Solution



Business users get simple, personalized role selection through intelligent and needs-based role recommendations

Approvers get better request context through descriptive, auto-generated request reason recommendations

Benefits



Increased user productivity and business agility through quicker systems access



Increased resilience to compliance and security threats through more accurate access provisioning

How it works

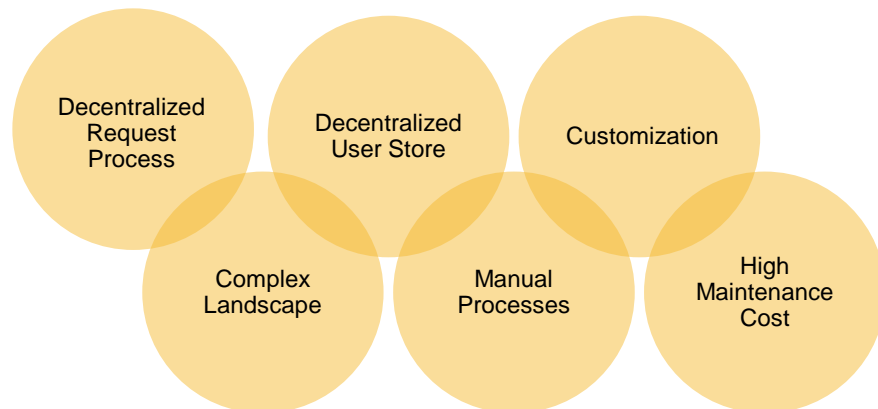
- **Machine Learning Recommendation System** for accurate, peer-based recommendations
- **Explainable AI** for transparent recommendations and user trust promotion
- **Natural Language Processing & Generation** for improved business needs capturing and an intuitive business user experience
- **Fully integrated** into existing SAP core Access Governance solutions

Change is a Journey, Not a Race!

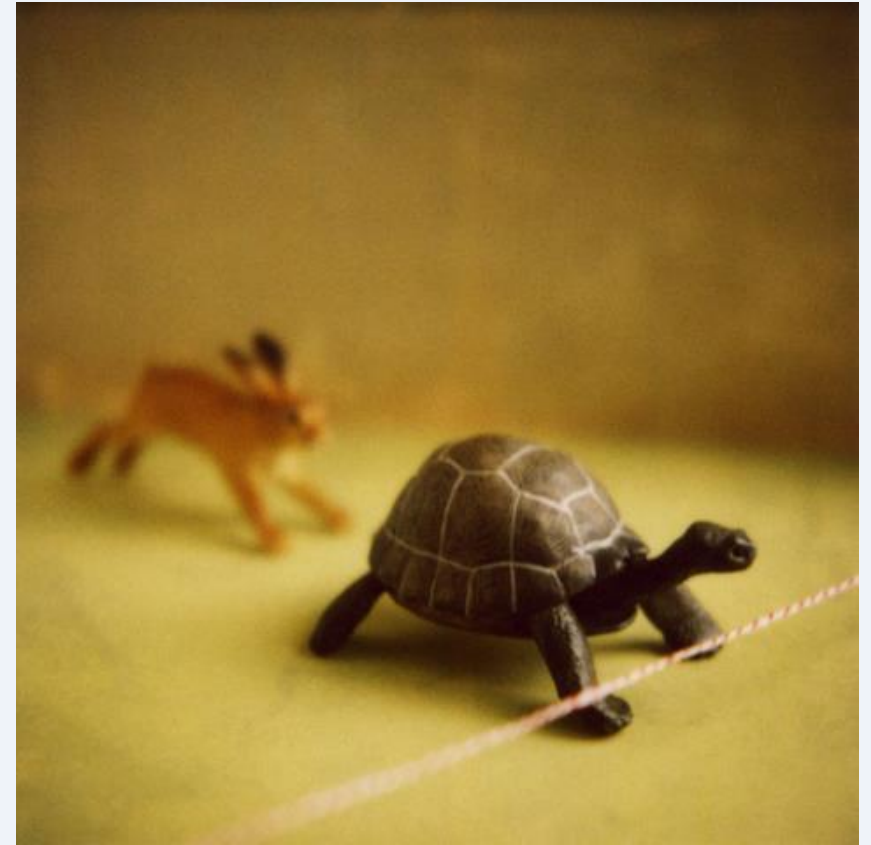
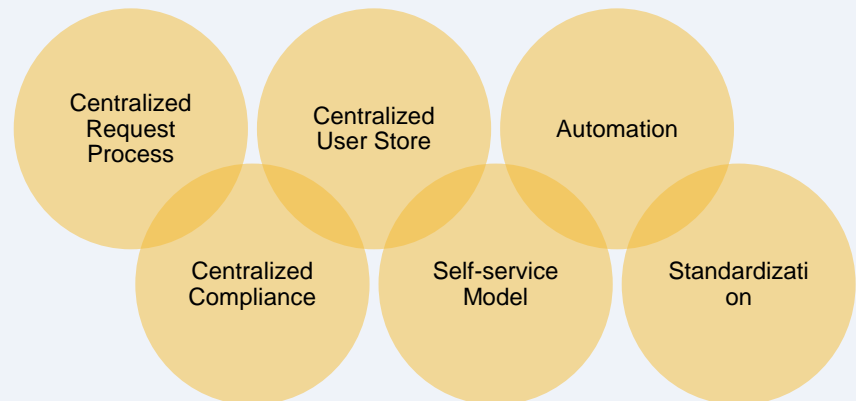


“I want to do it all at once! Let’s immediately transform our Identity and Access processes to be fully Self Service, with 100% business participation and completely Automated by the end of the year”

Customers need to evolve at a rate that allows them to incorporate functionality, business process change and gain business buy-in & participation at a speed that aligns with their ability to manage change.



Road Map

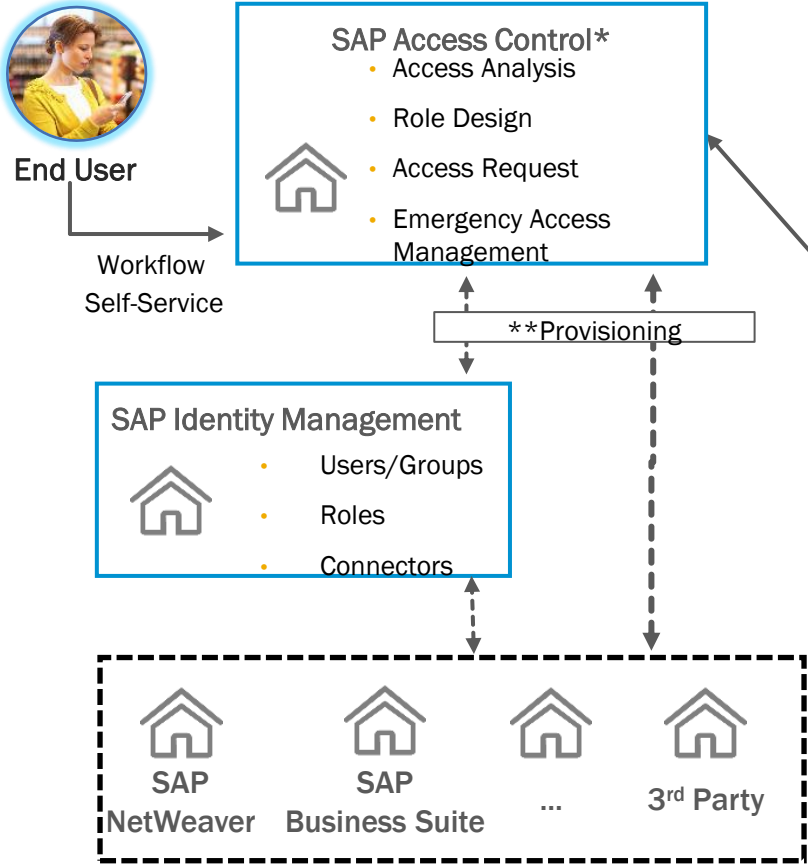


Making Access Provisioning a One Stop Shop - Connectivity and Integration Options



SAP Cloud Identity Access Governance Connectivity

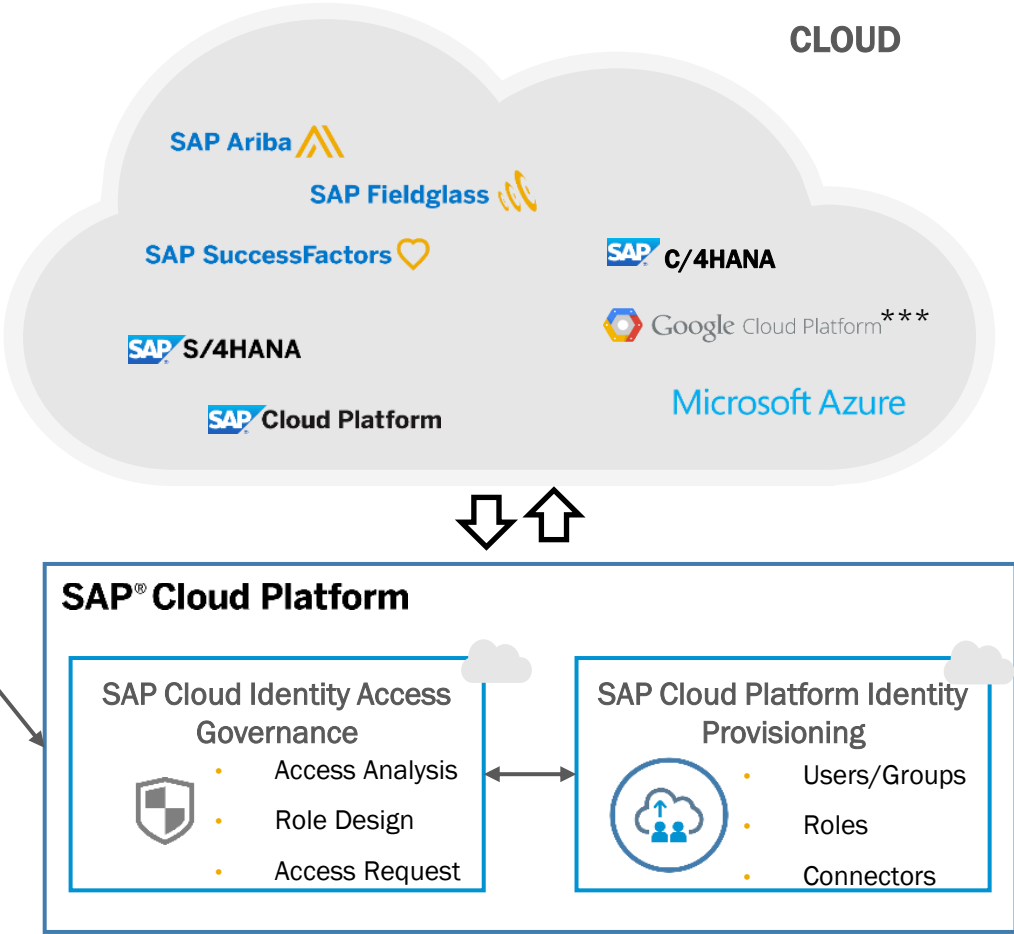
ON-PREMISE LANDSCAPE



Firewall

Cloud IAG Bridge*

CLOUD

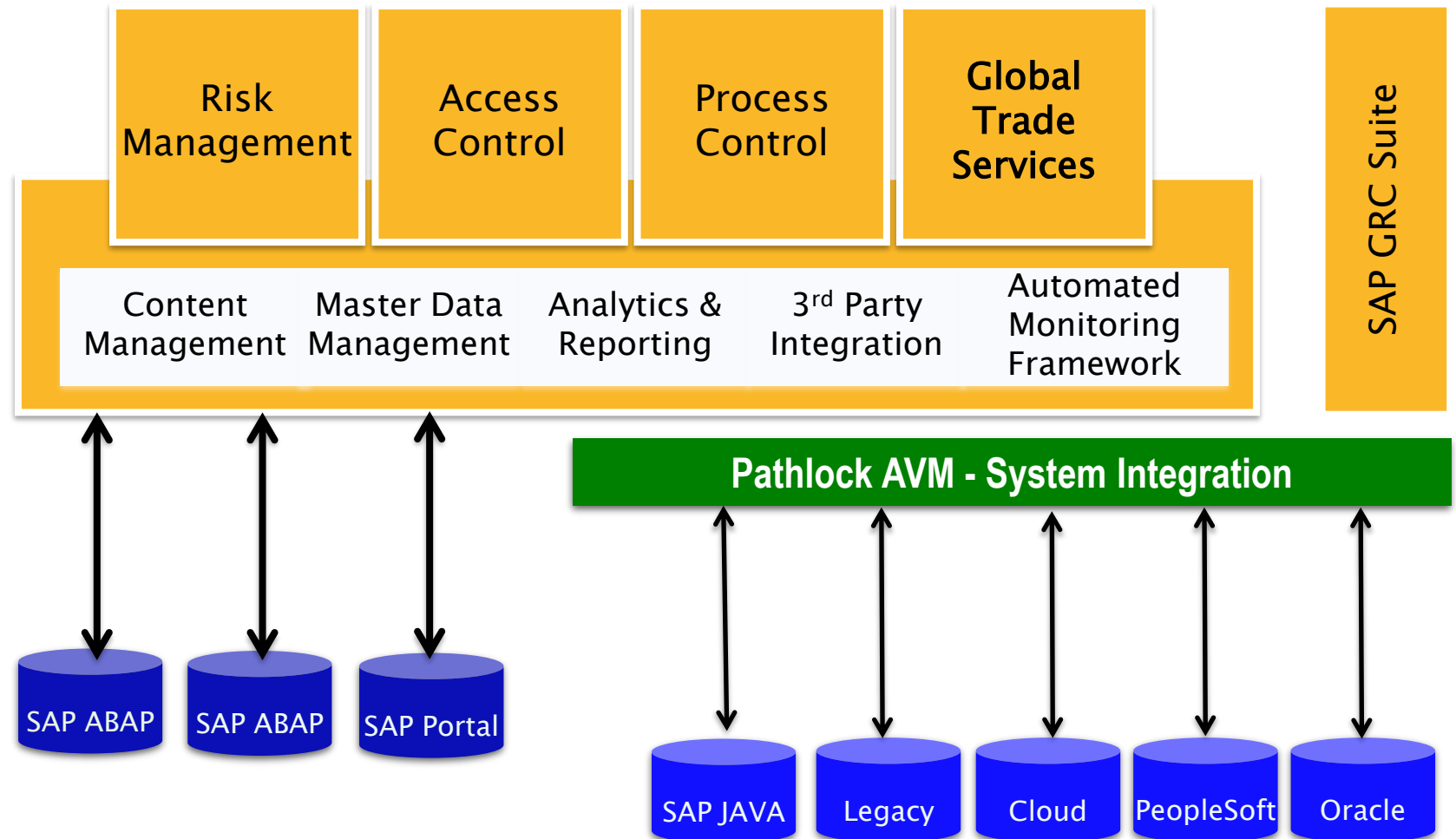


*SAP Access Control 12 and above

Optional. *Coming

SAP Access Violation Management by Pathlock – System Integration Edition

- Extend the capabilities of SAP Access Control across additional business applications and IT systems, eliminating administrative silos and enabling a more complete picture of user access across the organization.
- SAP Access Violation Management enables real-time risk analysis and provisioning, user access reviews, role management, and emergency access management to on-premise and cloud-based enterprise applications.



Wrap Up

Where to Find More Information

https://help.sap.com/docs/SAP_IDENTITY_MANAGEMENT/4773a9ae1296411a9d5c24873a8d418c/1c2d07aa6ed545a2a47b2b2153a965fe.html?locale=en-US

- SAP Identity Management Configuration Guide

https://help.sap.com/doc/4835e84042834e6c96bfa35f5d7609aa/1902/en-US/AC12%20to%20IAG%20Bridge_Integration.pdf

- Bridge: Access Control 12.0 with SAP Cloud Identity Access Governance Integration Guide

<https://help.sap.com/doc/a877d9f274d3471c9ef107e7b9fa1eef/12.0.03/en-US/loio9e08a4211c104a9696cdfccdc9bb3c8.pdf>

- SAP GRC AC 12.0 Admin Guide:

<https://help.sap.com/viewer/e739622ded9b4d92964c6a0f50b5f90e/latest/en-US/083fa2619ed24382ae21f664ba390f45.html>

- SAP IAG Release Notes

https://documentation.sailpoint.com/connectors/sap/grc/help/integrating_sap_grc/connecting_sap_grc_sailpoint.html

- Connecting SailPoint and SAP GRC

Key Points to Take Home

- In today's Security world a focus needs to be placed on establishing processes and implementing tools that foster “Compliant Provisioning” rather than just “Provisioning” solutions.
- There are multiple applications that exist to help address the “Compliant Provisioning” challenges customer face. Choosing the right application is essential! And sometimes it might require multiple applications working together capitalizing on their specific strengths.
- Every customer needs to have a consistent Compliant Provisioning Life Cycle of a user that is supported by Automation and User Self Service Security processes.
- It is not just about SAP! Companies need to have consistent Compliant Provisioning processes and tools that connect to and manage all landscapes.
- Conquering the challenge of Compliant Provisioning is an evolutionary process. Things are ever changing, Having a Roadmap that focuses on improving Automation, Controls, and evolving towards User Self-Service are the keys to success.

Thank you! Any Questions?



LinkedIn: <http://www.linkedin.com/in/jamesroeske/>

Twitter: <http://twitter.com/Roeskinator>

Please remember to complete
your session evaluation.

SAPinsider



SAPinsider.org

PO Box 982Hampstead, NH 03841
Copyright © 2023 Wellesley Information Services.
All rights reserved.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies. Wellesley Information Services is neither owned nor controlled by SAP SE.

SAPinsider comprises the largest and fastest growing SAP membership group worldwide, with more than 750,000 global members.
